Whitstable & Seasalter Endowed Church of England (Aided) Junior School

Mobile and Smart Technology Policy

This policy reflects our schools vision

LET YOUR LIGHT Shine
Matthew 5:14-16

Love ★ Joy ★ Goodness ★ Resilience ★ Trust

Reviewer	Headteacher
Reviewed	March 2024
Date of Next Review	March 2026
Headteacher Signature	Diane R Clements
Chair of Governors Signature	EM Taylor

This policy has been written by Whitstable and Seasalter Endowed church of England (Aided) Junior School, involving staff, pupils and parents/carers, building on Kent County Councils Education Safeguarding Service's mobile and smart technology policy template, with specialist advice and input as required.

It takes into account the DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage, 'Working Together to Safeguard Children', 'Behaviour in Schools Advice for headteachers and school staff', 'Searching, screening and confiscation at school' and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.

The purpose of this policy is to safeguard and promote the welfare of all members of our community when using mobile devices and smart technology.

The Whitstable and Seasalter Endowed Church of England (Aided) Junior School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm when using mobile and smart technology.

As outlined in our Child Protection Policy, the Designated Safeguarding Lead (DSL), Ellen Taylor (Headteacher) is recognised as having overall responsibility for online safety.

This policy applies to all access to and use of all mobile and smart technology on site; this includes but is not limited to mobile/smart phones and personal devices such as tablets, e-readers, games consoles and wearable technology, such as smart watches and fitness trackers, which facilitate communication or have the capability to record sound and/or images.

This policy applies to pupils, parents/carers and all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy).

1. Links with other policies

This policy links with several other policies, practices and action plans, including but not limited to:

- Anti-bullying policy
- Acceptable Use Policies (AUP)
- Behaviour and discipline policy
- Cameras and image use policy
- Child protection policy
- Staff code of conduct
- Confidentiality policy
- Data security
- Online Safety
- Social media
- Searching, screening and confiscation policy

2. Safe use of mobile and smart technology expectations

The Whitstable and Seasalter Endowed Church of England (Aided) Junior School recognises that use of mobile and smart technologies is part of everyday life for many pupils, staff and parents/carers.

Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of our community are advised to:

- take steps to protect their personal mobile phones or other smart devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on personal phones or devices.

Mobile devices and other forms of smart technology are not permitted to be used in specific areas on site; this includes changing spaces, toilets and swimming pools (if visiting other sites).

The sending of abusive or inappropriate messages or content, including via personal mobile devices and/or smart technology is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and child protection policies.

All members of the Whitstable and Seasalter Endowed Church of England (Aided) Junior School community are advised to ensure that their personal mobile and smart technology devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.

3. School provided mobile phones and devices (e.g. laptops/tablets)

Staff providing formal remote/online learning will do so using school provided equipment in accordance with our Acceptable Use Policy (AUP)/remote learning AUP.

School devices (laptops, tablets) will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff and/or pupils.

School devices will always be used in accordance with our staff code of conduct/behaviour policy, online safety, acceptable use of technology policy and other relevant policies.

Where staff and/or pupils are using school provided devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.

4. Staff use of mobile and smart technology

Members of staff will ensure that use of any mobile and smart technology, including personal phones, wearable technology and other mobile/smart devices, will take place in accordance with the law, as well as relevant school policy and procedures, including confidentiality, child protection, data security, staff behaviour/code of conduct and Acceptable Use Policies.

Staff will be advised to:

- Keep personal mobile and smart technology devices in a safe and secure place (locked in a locker/drawer) during lesson time.
- Keep personal mobile phones and devices switched off or set to 'silent' or 'do not disturb' modes during lesson times.
- Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
- Not use personal mobile or smart technology devices during teaching periods, unless written permission has been given by SLT, such as in emergency circumstances.
- Ensure that any content bought onto site via personal mobile and smart technology devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal mobile and smart technology devices for contacting pupils or parents and carers.

- Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL/Headteacher.
- Staff will only use school provided equipment (not personal devices):
- to take photos or videos of pupils in line with our image use policy.
- to work directly with pupils during lessons/educational activities.
- to communicate with parents/carers.

Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the Headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy and/or remote learning AUP.

If a member of staff breaches our policy, action will be taken in line with our staff code of conduct, child protection policy and/or allegations policy.

If a member of staff is thought to have illegal content saved or stored on a personal mobile or other device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted, and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

5. Learners' use of personal devices and mobile phones

5.1 Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

5.2 Whitstable & Seasalter Endowed Church of England (Aided) Junior School expects learners' personal devices and mobile phones to be switched off at all times when in school.

5.3 Pupils will keep their mobile phones switched off and hand it to a teacher who will keep it in a safe, secure place. If they use these devices in school time without teacher permission, they will be confiscated and returned to parents. Pupils will not be permitted to bring the device into school again for the remainder of the term.

5.4 In exceptional circumstances, agreed by the headteacher, if a learner needs to contact his/her parents or carers they will be allowed to use the school phone in the office and this would usually be done by an adult but an adult will always supervise. Parents are advised to contact their child via the office; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher.

5.5 Mobile phones or personal devices will not be used by learners during lessons or formal educational time.

5.6 Mobile phones or personal devices will not be used by learners during lessons or formal educational time.

5.7 If a learner requires access to a personal device in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the Headteacher prior to use being permitted.

5.7.1 Any decision regarding allowing access to personal devices in exceptional circumstances will be documented and recorded by the school in the Online Safety file. A Risk Assessment will also be carried out.

5.7.2 Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the learner and their parents carers before use is permitted.

5.8 Mobile phones and personal devices must not be taken into examinations.

5.8.1 Learners found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the

appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

5.9 Any concerns regarding learners' use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour.

5.9.1 If a learner breaches the policy, the phone or device will be confiscated and held in a secure place.

5.9.2 Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy.

5.9.3 Searches of mobile phone or personal devices will be carried out in accordance with our policies.

5.9.4 Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.

5.9.5 Mobile phones and devices that have been confiscated will be released to parents/ carers at the end of that day and we will recommend imposing sanctions on their mobile phone use for the remainder of the school term.

5.9.6 Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.

5.9.7 Concerns regarding policy breaches by learners will be shared with parents/carers as appropriate.

5.9.8 If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

6. Searching, screening and confiscation of electronic devices

Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.

Where there are any concerns regarding pupils' use of mobile or smart technology or policy breaches, they will be dealt with in accordance with our existing policies, including anti-bullying, child protection, online safety and behaviour.

Staff may confiscate a pupils' personal mobile or smart technology device if they believe it is being used to contravene our child protection or behaviour policy.

Personal mobile or smart technology devices that have been confiscated will be held in a secure place- (the school office) and released to parents/carers at the end of the day.

Where a concern involves a potentially indecent image or video of a child, staff will respond in line with our child protection policy and will confiscate devices, avoid looking at any content, and refer the incident to the Designated Safeguarding Lead or Online Safety DSL urgently as they will be most appropriate person to respond.

If there is suspicion that data or files on a pupil's personal mobile or smart technology device may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation

If deemed to be necessary and appropriate, searches of personal mobile or smart technology devices may be carried out in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance.

Staff will respond in line with our child protection policy and follow the most appropriate safeguarding response if they find images, data or files on a pupil's electronic device that they reasonably suspect are likely to put a person at risk.

The Designated Safeguarding Lead or DDSL will always be informed of any searching incidents where authorised members of staff have reasonable grounds to suspect a pupil was in possession of prohibited items, as identified in our behaviour policy.

The Designated Safeguarding Lead or DDSL will be involved without delay if staff believe a search of a pupil's personal mobile or smart technology device has revealed a safeguarding risk.

In exceptional circumstances and in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so:

In determining whether there is a 'good reason' to examine images, data or files, the Executive Headteacher or an authorised member of staff will need to reasonably suspect that the images, data or files on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.

In determining whether there is a 'good reason' to erase any images, data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable.

If the data or files are not suspected to be evidence in relation to an offence, the headteacher or an authorised member of staff may delete the images, data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves.

If the headteacher or a member of staff finds any data or files that they suspect might constitute a specified offence, they will be delivered to the police as soon as is reasonably practicable.

7. Visitors' use of mobile and smart technology

Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:

- They have read and signed the Visitor & Volunteer Acceptable Use Policy (AUP).
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection.

If visitors require access to mobile and smart technology, for example when working with pupils as part of multi-agency activity, this will be discussed with the Headteacher prior to use being permitted.

Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school. This may include undertaking appropriate risk assessments if necessary.

Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or DDSL of any breaches of our policy.

8. Policy monitoring and review

Technology evolves and changes rapidly. The Whitstable and Seasalter Endowed Church of England (Aided) Junior School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.

We monitor internet and technology use taking place via all school provided devices and systems and regularly evaluate online safety mechanisms to ensure this policy is consistently applied. Full information about the appropriate filtering and monitoring systems in place are detailed in our child protection policy and online safety policy. Any issues identified as a result of our monitoring approaches will be incorporated into our action planning.

All members of the community will be made aware of how the school will monitor policy compliance through our Acceptable Use Policy and Online Safety Policy.

9. Responding to policy breaches

All members of the community are informed of the need to report policy breaches or concerns in line with existing school policies and procedures. This includes child protection, behaviour policy, whistleblowing and online safety policies.

Where pupils breach this policy appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy and concerns will be shared with parents/carers as appropriate.

We will respond in line with our child protection policy, if there is a concern that a child is at risk of harm.

After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

We require staff, parents/carers and pupils to work in partnership with us to resolve issues.

All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.

Pupils' parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

If we are unsure how to proceed with an incident or concern, the DSL or DDSL will seek advice from Kent County Councils Education Safeguarding Service or other agency in accordance with our child protection policy.

10. Use of Social Media

10.1 Expectations

10.1.1 The expectations regarding safe and responsible use of social media applies to all members of Whitstable & Seasalter Endowed Church of England (Aided) Junior School's community.

10.1.2 The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger apps or services.

10.1.3 All members of our school community are expected to engage in social media in a positive and responsible manner.

10.1.4 All members of the school community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

10.1.5 We will control learner and staff access to social media whilst using school-provided devices and systems on site. Staff will not use school provided devices or computers to access social media, unless they are managing the school's official social media channels.

10.1.6 The use of social media during school for personal use is not permitted for staff.

10.1.7 The use of social media during school hours for personal use is not for learners. We will also recommend to our learner to minimise social media use at home as the majority of these apps/websites are intended for children over 13 years old.

10.1.8 Inappropriate or excessive use (usage which impacts upon their ability to fulfil their work requirements) of social media during school hours or whilst using school or personal devices may result in removal of internet access and/or disciplinary action.

10.1.9 Concerns regarding the online conduct of any member of the school community on social media, will be reported to the Headteacher and will be managed in accordance with existing policies, including anti-bullying, allegations against staff, behaviour and child protection.

10.2 Staff personal use of social media

10.2.1 The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

10.2.2 Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our Staff Code of Conduct and in our Online Safety Policy and Staff AUP.

10.2.3 Any complaint about staff misuse or policy breaches will be referred to the headteacher/manager, in accordance with our Staff Conduct Policy.

10.2.4 Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

10.2.5 If appropriate, disciplinary, civil and/or legal action will be taken in accordance with our staff Code of Conduct.

10.3 Reputation

10.3.1 All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school community.

10.3.2 Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

10.3.3 All members of staff are advised to safeguard themselves and their privacy when using social media services. Advice will be provided to staff via staff training and by

sharing appropriate guidance and resources on a regular basis. This will include, but is not limited to:

10.3.3.1 Setting appropriate privacy levels on their personal accounts/sites.

10.3.3.2 Being aware of the implications of using location sharing services.

10.3.3.3 Opting out of public listings on social networking sites.

10.3.3.4 Logging out of accounts after use.

10.3.3.5 Using strong passwords.

10.3.4 Ensuring staff do not represent their personal views as being that of the setting.

10.3.5 Members of staff are encouraged not to identify themselves as employees of the school on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.

10.3.6 All members of staff are encouraged to carefully consider the information, including text and images, they share and post online. Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies, and the wider professional and legal framework.

10.3.7 Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues, will not be shared or discussed on social media sites.

10.3.8 Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents/carers

5.1.1 Staff will not use any personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.

5.1.2 All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media sites, applications or profiles.

5.1.3 Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and the Headteacher.

5.1.4 Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff.

5.1.5 If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

5.1.6 Any communication from learners and parents received on personal social media accounts will be reported to the Headteacher.

8.3 Learners' use of social media

8.3.1 Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach via age appropriate sites and resources.

8.3.2 We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.

8.3.3 Learners will be advised:

- to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
- to only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
- to use safe passwords.
- to use social media sites which are appropriate for their age and abilities.
- how to block and report unwanted communications.
- how to report concerns on social media, both within the setting and externally.

8.3.4 Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying, child protection and behaviour.

8.3.5 The DSL (or deputy) will respond to online safety concerns involving safeguarding or child protection risks in line with our child protection policy.

8.3.6 Sanctions and/or pastoral/welfare support will be implemented and offered to learners as appropriate, in line with our behaviour policy. Civil or legal action will be taken if necessary.

8.3.7 Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

8.4 Official use of social media

8.4.1 The school's official social media channels are Facebook and Twitter.

8.4.2 The official use of social media sites by the school only takes place with clear educational or community engagement objectives and with specific intended outcomes.

8.4.3 The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.

8.4.4 Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

8.4.5 Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.

8.4.6 Staff use setting provided email addresses to register for and manage official social media channels.

8.4.7 Official social media sites are suitably protected and, where possible, they are linked to our website pages.

8.4.8 Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

8.4.9 Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.

8.4.10 All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.

8.4.11 Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

8.4.12 Only social media sites which have been risk assessed and approved as suitable for educational purposes will be used.

8.4.13 Any official social media activity involving learners will be moderated if possible.

8.4.14 Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.

8.4.15 We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels and we will make efforts to share this information with these families as well, via telephone and written letters.

8.4.16 Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.

8.4.17 If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:

- Sign our social media acceptable use policy. (AUP)
- Be aware they are an ambassador for the setting.
- Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure appropriate consent has been given before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any private/direct messaging with current or past learners or parents/carers.
- Inform their line manager, the DSL (or deputy) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

9. Responding to policy breaches

9.1 All members of the community will be made aware of how the school will monitor policy compliance through AUPs for stakeholders in school and communication to parents and carers at home.

9.2 All members of the community are informed of the need to report policy breaches or concerns in line with existing policies and procedures. This may include Child Protection policies, the Anti-Bullying Policy and the Online Safety Policy.

9.3 All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.

9.4 Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

9.5 We require staff, parents/carers and learners to work in partnership with us to resolve issues.

9.6 If appropriate, after any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

9.7 If we are unsure how to proceed with an incident or concern, the Headteacher (DSL) will seek advice from the Education People's Education Safeguarding Service (www.theeducationpeople.org/products/safeguarding/education-safeguarding-team-contacts/) or other agency in accordance with our child protection policy.

9.8 Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm.